

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
INTERNATIONAL CHAUFFEURED SERVICE, INC.,

Plaintiff,

- against -

MEMORANDUM AND ORDER

FAST OPERATING CORP., d/b/a CARMEL CAR &
LIMOUSINE SERVICE, and JOHN DOES 1-100,

11 Civ. 2662 (NRB)

Defendants.

-----X
NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE

Plaintiff International Chauffeured Service, Inc. brings this lawsuit against defendants Faster Operating Corp., d/b/a Carmel Car & Limousine Service ("Carmel"), and John Does 1-100, alleging a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (the "CFAA"), and asserting state common law claims of misappropriation of trade secrets and unfair competition. Presently before us is Carmel's motion to dismiss the complaint for failure to state a claim upon which relief can be granted pursuant to Federal Rule of Civil Procedure 12(b)(6).

For the reasons set forth herein, Carmel's motion is granted.

BACKGROUND¹

Plaintiff is a corporation organized under the laws of Delaware, with its principal place of business in New York. Since 1999, it has been operating a global chauffeured car service, matching passengers with drivers upon request. In offering this service, plaintiff relies upon a proprietary database -- created over a period of more than ten years -- containing potential pick-up and drop-off locations, as well as the pricing information for the numerous possible permutations of the two.

Carmel is a New York corporation, with its principal place of business also in New York. Carmel had been operating its own chauffeured car service in New York, New Jersey, and Connecticut, when it approached plaintiff in late 2007 or early 2008 about purchasing plaintiff's business. Carmel subsequently decided not to pursue the transaction but expanded its operations nationwide in 2009. Like plaintiff, Carmel also utilizes a database of pick-up and drop-off locations and prices.

Plaintiff alleges that Carmel's database is a "carbon copy" of its own, containing "typos, abbreviations, and colloquial references to geographical locations," as well as pricing

¹ Except where noted, these facts are derived from the First Amended Complaint (the "FAC"), the allegations of which we accept as true for purposes of the motion to dismiss.

information, identical to those found in plaintiff's database.² (FAC ¶ 12.) Plaintiff infers from the identity of the two databases that Carmel accessed plaintiff's restricted and proprietary server without authorization and copied its database, which resides on a network of three computers at plaintiff's principal place of business, though it does not allege when such access may have occurred.

Plaintiff alleges that, "[a]s a result of Carmel's unauthorized accessing" of its server, it needed "to investigate and remedy the effects of that unauthorized access." (Id. ¶ 24.) The security investigation was performed by LimoSys Software LLC ("LimoSys"), the developer of the database, between October 19 and October 21 of 2009 at a cost of \$1413. Subsequently, plaintiff tasked Aaron Shmuel, one of its employees, to monitor its servers and networks "for any indications of further unauthorized access." (Aff. in Supp. of Pl.'s First Am. Compl. ("Oren Aff.") ¶ 7.) Shmuel engaged in these monitoring activities for three hours a day until June 2010, when he cut back to one hour per day. Plaintiff instructed Shmuel to discontinue the monitoring in November 2010, and it attributes "roughly" \$13,900 of Shmuel's salary over the time period from

² Carmel's database apparently differs from plaintiff's with respect to entries for New York, New Jersey, and Connecticut, which Carmel presumably developed on its own prior to its expansion.

November 2009 to November 2010 to that monitoring. (Id.)³ Plaintiff further alleges that Carmel's misappropriation of the database has resulted in a substantial loss of plaintiff's business, which loss it values at \$5,919,781.

Plaintiff brought suit on April 19, 2011, alleging a violation of the CFAA, misappropriation of trade secrets, and unfair competition, and seeking to recover the above costs.

DISCUSSION

I. Legal Standards

When deciding a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure, the Court must accept as true all well-pleaded facts alleged in the complaint and draw all reasonable inferences in plaintiff's favor. See Kassner v. 2nd Ave. Delicatessen, Inc., 496 F.3d 229, 237 (2d Cir. 2007). We need not, however, accept

³ The FAC asserts that plaintiff spent \$7077 on "payroll costs for an employee who spent at least two-thirds of his time in the year preceding October 21, 2009 monitoring [plaintiff's] network for suspicious activity and intrusions." (FAC ¶ 24.) In a March 20, 2012 teleconference with the parties, the Court noted that, if the allegations in the FAC were to be taken at face value, because these costs for the year preceding October 21, 2009 were claimed to be a "result of Carmel's unauthorized access[]" of plaintiff's server, the FAC -- which does not allege even a month in which the access is supposed to have occurred -- would be implying that it learned that its servers were accessed sometime in 2008. We also noted that, if that were the case, plaintiff would run afoul of the statute of limitations on its CFAA claim. See 18 U.S.C. § 1030(g) (providing a two-year statute of limitations). Plaintiff subsequently filed an affidavit asserting that it had actually incurred a different set of monitoring costs as a result of defendant's intrusion -- as described above -- and attributing the allegations in the FAC to "a linguistic misunderstanding." (Oren Aff. ¶ 8.) Defendant has not objected to the submission of the affidavit, and so we utilize the facts alleged therein for the purposes of this motion, even though they conflict with those contained in the FAC.

as true mere "conclusions of law or unwarranted deductions of fact." First Nationwide Bank v. Gelt Funding Corp., 27 F.3d 763, 771 (2d Cir. 1994) (internal quotation marks omitted).

A complaint must contain "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (citing Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). Where a plaintiff has not "nudged [its] claims across the line from conceivable to plausible, [its] complaint must be dismissed." Twombly, 550 U.S. at 570.

II. The Computer Fraud and Abuse Act

The CFAA makes unlawful, among other actions not relevant here, "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage." 18 U.S.C. § 1030(a)(5)(B). While the CFAA is primarily a criminal statute, a civil cause of action is permitted against any such violator, provided that the offense caused "loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value," or other consequences not relevant here. Id. § 1030(c)(4)(A)(i)(I), (g).

A. Whether Carmel Accessed a "Protected Computer"

Carmel begins its volley of attacks on the sufficiency of the FAC by arguing that plaintiff has not alleged that Carmel accessed a "protected computer." In particular, Carmel asserts

that plaintiff has failed to allege, first, that Carmel accessed any computer at all and, second, that plaintiff operates in interstate commerce, which is required for its computers to be protected by the CFAA, see 18 U.S.C. § 1030(e)(2)(B).

Carmel's first argument is utterly baseless. The CFAA defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions." Id. § 1030(e)(1). Plaintiff alleges that Carmel accessed its database, which "was on a restricted and proprietary server," and that the database could only have been accessed "by gaining unauthorized access to the . . . [s]ervers." (FAC ¶¶ 14, 22.) The Court is fully aware that, in this context, the term "server" refers to a computer or network of computers that hosts data to be accessed from other sources,⁴ making these allegations more than sufficient for purposes of the CFAA. Even if we were not aware of what a server was, however, plaintiff specifically alleges that the accessed database "resides on a network of computers." (Id. ¶ 19.) It is beyond absurd to argue that plaintiff could be alleging anything other than that Carmel accessed a computer when it accessed plaintiff's database.

⁴ See, e.g., Merriam-Webster, <http://mw1.merriam-webster.com/dictionary/server> ("a computer in a network that is used to provide services (as access to files or shared peripherals or the routing of e-mail) to other computers in the network").

Carmel's second argument also fails. So long as the computer at issue is "used to conduct business across state lines," it qualifies as "protected." Dedalus Found. v. Banach, No. 09 Civ. 2842, 2009 U.S. Dist. LEXIS 98606, at *7 (S.D.N.Y. Oct. 16, 2009) (citing Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1033-34 (N.D. Ill. 2008) ("[I]t suffices to state the computer was used for the business and the business operated in two different states.")); see also Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314, 318-19 (D. Conn. 2008) (finding the fact that defendant had an office in a state other than where its principal place of business was located sufficient to satisfy the interstate commerce requirement). Here, plaintiff alleges that the database resides on a computer network that is physically located at plaintiff's principal place of business, which is in New York. (FAC ¶¶ 4, 19.) It further alleges that the database contains permutations of pick-up and drop-off locations "throughout the United States and the world," and that "the majority of the price quotes" it issues using that data is "made to customers outside of the State of New York." (Id. ¶¶ 8, 20.) The requirement that the computer be utilized in interstate commerce is fully satisfied by the allegations in the FAC.⁵

⁵ The FAC also alleges that plaintiff provides its services to visitors to its website. (FAC ¶¶ 6-7.) To the extent the database is utilized to provide

B. Whether Carmel Caused a "Loss" of \$5000 or More

The second threshold element of plaintiff's CFAA claim that Carmel challenges is the requirement that the violation have caused a "loss" of at least \$5000. The CFAA defines a "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Courts construe "loss" narrowly, B.U.S.A. Corp. v. Ecogloves, Inc., No. 05 Civ. 9988, 2009 U.S. Dist. LEXIS 89035, at *18 (S.D.N.Y. Sept. 28, 2009), and the term "includes only costs actually related to computers," Garland-Sash v. Lewis, No. 05 Civ. 6827, 2011 U.S. Dist. LEXIS 143626, at *8-9 (S.D.N.Y. Dec. 6, 2011). Courts have interpreted the term to mean "any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made." E.g., id. at *9-10 (quoting Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004), aff'd 166 F. App'x 559 (2d Cir. 2006)). The case law in this Circuit thus requires a cost

services to those customers, (id. ¶ 28), it affects interstate commerce. See Dedalus Found., 2009 U.S. Dist. LEXIS 98606, at *7.

constituting a loss to be directed in some way at the effects of the prior intrusion, not at those of some potential future offense. See Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010).

The CFAA requires that, for consequential damages to be included in the loss amount, they must be the result of an interruption in service. See 18 U.S.C. § 1030(e)(11). Because it is undisputed that the alleged unauthorized access of plaintiff's database did not cause such an interruption, the \$5,919,781 in business plaintiff alleges it has lost does not count toward this threshold requirement. See Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010); Nexans, 319 F. Supp. 2d at 477-78.

Also without controversy is that costs of the investigation conducted by LimoSys do count toward the threshold; because LimoSys was hired "to investigate and remedy the effects of [the] unauthorized access," (FAC ¶ 24), the expense attributable to that work is precisely the kind the CFAA contemplates as constituting loss. See Kaufman v. Nest Seekers, LLC, No. 05 Civ. 6782, 2006 U.S. Dist. LEXIS 71104, at *24-25 (S.D.N.Y. Sept. 27, 2006) (finding that "the costs involved in investigating the damage to the computer system may constitute such a loss," even when no damage is found).

The cost of LimoSys's investigation, however, was only \$1413, insufficient to meet the \$5000 threshold. The sufficiency of the loss allegations thus turns on whether the expense attributable to Shmuel's monitoring of plaintiff's networks "for any indications of further unauthorized access," (Oren Aff. ¶ 7), is a "loss" for purposes of the CFAA.

Such monitoring does not fall within any of the categories of loss that have been identified as contemplated by Section 1030(e)(11). Courts have found that "prophylactic" measures that do not "identify and address damage caused by the security breach that had already taken place," even if prompted by that earlier breach, "probably do[] not fall within the statutory definition of 'loss.'" Univ. Sports, 725 F. Supp. 2d at 388;⁶ see also Cohen v. Gerson Lerman Grp., Inc., No. 09 Civ. 4352, 2011 U.S. Dist. LEXIS 104551, at *23 (S.D.N.Y. Sept. 15, 2011); cf. Tyco Int'l (US) Inc. v. Doe, No. 01 Civ. 3856, 2003 U.S. Dist. LEXIS 25136, at *9 (S.D.N.Y. Aug. 29, 2003) ("While . . . the CFAA allows recovery for losses beyond mere physical damage to

⁶ University Sports involved two audits, only one of which the court deemed a loss for purposes of the CFAA. The first "sought to identify ways to improve the database's security systems," while the second "sought to identify evidence of the breach, assess any damage it may have caused, and determine whether any remedial measures were needed to resecure the network." Univ. Sports, 725 F. Supp. 2d at 388. The former -- the audit not deemed a loss -- is prospective, the latter retrospective. In letter briefing submitted following the submission of plaintiff's affidavit, plaintiff attempts to characterize Shmuel's monitoring as akin to the second audit in University Sports. As explained further below, however, the monitoring of plaintiff's servers is much closer in kind to an improvement to plaintiff's security going forward than it is to an assessment and rectification of damage already caused.

property, the additional types of damages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff's computer system or to resecure the system in the wake of a spamming attack." (internal citation omitted)). In short, "loss," for the purposes of the CFAA, encompasses only "repair cost[s] or cost[s] associated with investigating the alleged damage." Bose v. Interclick, Inc., No. 10 Civ. 9183, 2011 U.S. Dist. LEXIS 93663, at *12 (S.D.N.Y. Aug. 17, 2011).

Tasking Shmuel to monitor plaintiff's networks is not a cost of the type that may be recovered. The monitoring was an added security measure -- akin to installing a security camera in the aftermath of a break-in to ensure that evidence of future break-ins would be detected -- not a restoration of existing security measures or remedial in any other way. Although the monitoring may have been prompted by the alleged intrusion into plaintiff's servers,⁷ it was a precaution taken against future

⁷ We note, parenthetically, our skepticism that any costs associated with the monitoring are properly attributable to the alleged misappropriation of plaintiff's database. Plaintiff actually attributes the monitoring to "the uncertain results of [LimoSys's] investigation," (Oren Aff. ¶ 7), but we find even that causality difficult to credit. As noted earlier, the FAC alleges that plaintiff utilized two-thirds of an employee's time to monitor its network in the year preceding October 21, 2009. (FAC ¶ 24.) Plaintiff later submitted an affidavit attributing variously three hours and one hour a day of an employee's time to monitoring for the year after October 21, 2009. (Oren Aff. ¶ 7.) That affidavit explains the FAC's allegations as "due to a linguistic misunderstanding about the period in question with respect to Mr. Shmuel's salary costs," leading plaintiff's president to "provide[] [plaintiff's] counsel with salary records for periods preceding October 2009 rather than entirely subsequent to the unauthorized access at issue." (*Id.* ¶ 8.) These facts suggest that plaintiff, even prior to its learning of the

intrusions and is not an expense properly identified as a "loss" under the CFAA. Plaintiff has therefore not sufficiently alleged a \$5000 loss.

Having failed to establish this threshold requirement, plaintiff's CFAA claim is dismissed.

III. Plaintiff's State Law Claims

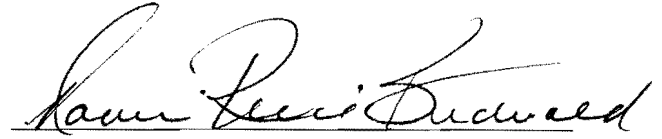
Plaintiff also asserts claims under New York common law for misappropriation of trade secrets and unfair competition. Our original jurisdiction in this case is based on the CFAA claim, and, having dismissed that claim, we "may decline to exercise supplemental jurisdiction over [the state] claim[s]." 28 U.S.C. § 1367(c). Indeed, it is policy in this Circuit that, "where all the federal claims have been dismissed at a relatively early stage, the district court should decline to exercise supplemental jurisdiction over pendent state-law claims." Astra Media Grp., LLC v. Clear Channel Taxi Media, LLC, 414 F. App'x 334, 337 (2d Cir. 2011); see also Marcus v. AT&T Corp., 138 F.3d 46, 57 (2d Cir. 1998). We adhere to this policy and dismiss plaintiff's state law claims without prejudice.

alleged security breach, utilized employees to monitor its computer systems. If that is the case, monitoring costs after October 21, 2009 are likely not fairly attributable to the alleged conduct because they would be a cost incurred in the regular course of plaintiff's business.

CONCLUSION

For the foregoing reasons, the motion (docket no. 15) is granted and the FAC is dismissed in its entirety.

Dated: New York, New York
April 13, 2012


NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE

Copies of the foregoing Order have been mailed on this date to the following:

Attorneys for Plaintiff

Brett E. Lewis, Esq.
David D. Lin, Esq.
Lewis & Lin, LLP
45 Main Street, Suite 818
Brooklyn, NY 11201

Attorney for Defendants

Steven J. Shanker, Esq.
The Shanker Law Firm
40 Fulton Street, 23rd Floor
New York, NY 10038